

DU2

COMMISSIONER FOR TALENTS

P.O. BOX 1450

ALEXANDRIA, VA 22313-1450

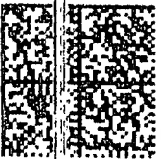
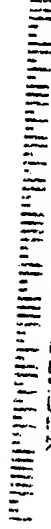
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS

AN EQUAL OPPORTUNITY EMPLOYER

FHIL580* 105917033 1603 08 06/22/04
 FORWARD TIME EXP RIN TO SEND
 :PHILIPS ELECTRONICS NO AMERICA
 345 SCARBOROUGH RD
 BRIARCLIFF MANOR NY 10510-2027

RETURN TO SENDER



0004202245 JUN 16 2004
MAILED FROM ZIP CODE 22202

UNITED STATES POSTAGE
 U.S. OFFICIAL MAIL
 PENALTY FOR
 PRIVATE USE \$300
 PRINTED BY
 PRINTER HOUSES



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/555,303	05/26/2000	Markus Feuser	PHD 99-096	3913

7590 06/16/2004
Philips Elcetronics North American Corp.
580 White Plains Rd.
Tarry town, NY 10591

EXAMINER

ARANI, TAGHI T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 06/16/2004

9

Please find below and/or attached an Office communication concerning this application or proceeding.

RECEIVED

JUN 25 2004

Technology Center 2100

Office Action Summary	Application No. 09/555,303	Applicant(s) FEUSER, MARKUS	
	Examiner Taghi T. Arani	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4-6 and 9-11 is/are pending in the application.
 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1, 4-6, 9-11 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

Art Unit: 2131

DETAILED ACTION

Claims 1-11 were pending for examination.

Claims 2-3, 7-8 are cancelled.

Claims 1, 4- 6, 9-11 are amended.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 and 6 are rejected under 35 U.S.C. 101 because claims 1 and 6 recite “ a data processing device which includes an integrated circuit which executes useful arithmetic cryptographic operations” and “ the integrated circuit” is randomly switched” between different modes of operation” and “the different modes of operation.... including at least two calculation methods... which produce an identical result while using different arithmetic approaches”.

the language of the claims raises a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claims 4-5, 9-11 are also rejected by virtue of their dependencies.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary

Art Unit: 2131

skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4-6, 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, Griffin, III et al, and Sprunk and further in view of Ohki et al.

As per (amended) claims 1, 4 6 and 9, Griffin is directed to a method for preventing compromise of secure data processing routines (i.e. a cryptographic operations) by a procedure known as a “clock attack”, see col. 1, lines 10-34. Griffin’s invention prevents clock attacks by providing a method that inhibits synchronization with externally generated instructions by preventing determination of the time of execution of a predetermined data processing routine in relation to occurrence of an externally observable event that precedes execution of the determined routine.

The method of Griffin includes step of randomly varying the duration between the occurrence of the externally observable event and the execution of the predetermined routine, see col. 1, lines 35-52.

Griffin’s invention implemented in a secure microprocessor executes a group of data processing routines (i.e. different modes of operation under random control), see col. 3, lines 1-36.

Griffin fails to teach a second clock signal derived from first clock signal under random control to be applied to the integrated circuit.

However, Sprunk discloses a secure microprocessor with reduced vulnerability to attack, see abstract, in which the secure microprocessor clock (i.e. first clock signal) is modulated (i.e. a second clock signal) in a substantially random fashion which eliminates the ability to predict the clock even if it is observable, see col. 1, lines 50-54.

Griffin-Sprunk fail to teach “two calculation methods which produce an identical result while using different arithmetic approaches”.

Art Unit: 2131

However, Ohki discloses an IC card chip wherein prior to executing an input data process of the IC card chip, the input data is transformed to thereby reduce the relation between the process data and the consumption current of the IC card chip, see abstract.

Ohki 's IC card includes a central processing unit for executing a data process in accordance with a program including one or more data process means each being a process instruction for giving an execution instruction to the central processing unit. The data processing means of Ohki comprises: a data transformed process means executing an operation OP1 on a transformed data H1 (which is the transformation of input data D1 by using a disturbance data Xi) and a data un-transforming processing means for executing an operation process OP2 which produces an identical value as the operation process OP1 for the input data D1. The teaching of Ohki suggests two calculation methods which produce an identical result while using different arithmetical approaches (recited in claims 1 and 6) and that a "dummy " operation (i.e. transforming input data using operation op1 on the disturbance data Xi) in which the IC card does not execute useful operations and un-transforming the transformed data (useful operation) wherein disturbance data (Xi) is rejected and not taken up in the results (recited in claims 4 and 9), see col. 4, lines 6-35, col. 6 line 10 through col 7, line 36.

It would have been obvious to one of ordinary skill in the art to employ secure microprocessor of Sprunk with clock signal modulation in secure data processing scheme of Griffin to preclude the observation of a clock signal and to render the observation of a portion of a clock signal useless for predicting the future operation, col. 1, lines 37-48 (Sprunk).

It would have been further obvious to one of ordinary skill in the art to modify Griffin's secure data processing routines to that of Ohki and Spunk to prevent both "clock attack" and

Art Unit: 2131

measuring and monitoring of the IC card consumption current (i.e. to prevent “Differential Power analysis”), see col. 1, lines 50-62 (Ohki et al.).

As per (amended) claims 5 and 10, Griffin teaches preventing the execution of a predetermined routine in response to a tamper detect counter, see abstract, see also col. 5, lines 12-18. that is, the integrated circuit does not execute arithmetic operations.

Allowable Subject Matter

Claim 11 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Amendment

Applicant's arguments filed on 3/25/2004 regarding the rejection of the claims 1, 4-6,9-11 under 35 U.S.C. 103() have been fully considered but they are not persuasive.

As per Applicant's arguments relating to Ohki et al. reference, the Applicant argues that “Ohki generally describes equipment that performs a single calculation method, not an integrated circuit that is randomly switched between at least two calculation methods.”, page 5, 4th paragraph.

The Examiner disagrees. As addressed in the rejection of claims 1 and 6 above, Ohki's data processing equipment performs various processes (calculation methods) in transforming and un-transforming the input data by using a disturbance data Xi .

The Examiner further responds that the Ohki et al. is a secondary reference in a 103 type rejection used in combination with clock frequency modulation of Sprunk (for randomly switching between “at least two calculation methods”.

Art Unit: 2131

Action is Final

THIS ACTION IS FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion


Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned is:

(703) 872-9306

Taghi Arani

Patent Examiner


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

USPTO TO PROVIDE ELECTRONIC ACCESS TO CITED U.S. PATENT REFERENCES WITH OFFICE ACTIONS AND CEASE SUPPLYING PAPER COPIES

In support of its 21st Century Strategic Plan goal of increased patent e-Government, beginning in June 2004, the United States Patent and Trademark Office (Office or USPTO) will begin the phase-in of its E-Patent Reference program and hence will: (1) **provide downloading capability of the U.S. patents and U.S. patent application publications cited in Office actions** via the E-Patent Reference feature of the Office's Patent Application Information Retrieval (PAIR) system; and (2) **cease mailing paper copies of U.S. patents and U.S. patent application publications with Office actions** (in applications and during reexamination proceedings) except for citations made during the international stage of an international application under the Patent Cooperation Treaty (PCT). In order to use the new E-Patent Reference feature applicants must: (1) obtain a digital certificate and software from the Office; (2) obtain a customer number from the Office; and (3) properly associate patent applications with the customer number. Alternatively, copies of all U.S. patents and patent application publications can be accessed without a digital certificate from the USPTO web site, from the USPTO Office of Public Records, and from commercial sources. The Office will continue the practice of supplying paper copies of foreign patent documents and non-patent literature with Office actions. Paper copies of cited references will continue to be provided by the USPTO for international applications during the international stage.

Schedule

June 2004	TCs 1600, 1700, 2800 and 2900
July 2004	TCs 3600 and 3700
August 2004	TCs 2100 and 2600

All U.S. patents and U.S. patent application publications are available on the USPTO web site. However, a simple system for downloading the cited U.S. patents and patent application publications has been established for applicants, called the E-Patent Reference system. As E-Patent Reference and Private PAIR require participating applicants to have a customer number, retrieval software and a digital certificate, all applicants are strongly encouraged to contact the Patent Electronic Business Center to acquire these items. To be ready to use this system by June 1, 2004, contact the Patent EBC as soon as possible by phone at 866-217-9197 (toll-free), 703-305-3028 or 703-308-6845 or electronically via the Internet at ebc@uspto.gov.

Other Options

The E-Patent Reference function requires the applicant to use the secure Private PAIR system, which establishes confidential communications with the applicant. Applicants using this facility must receive a digital certificate, as described above. Other options for obtaining patents which do not require the digital certificate include the USPTO's free Patents on the Web program (<http://www.uspto.gov/patft/index.html>). The USPTO's Office of Public Records also supplies copies of patents for a fee (<http://ebiz1.uspto.gov/oems25p/index.html>). Commercial sources also provide U.S. patents and patent application publications.

For complete instructions see the Official Gazette Notice, USPTO TO PROVIDE ELECTRONIC ACCESS TO CITED U.S. PATENT REFERENCES WITH OFFICE ACTIONS AND CEASE SUPPLYING PAPER COPIES, on the USPTO-web site.

**NOTICE OF OFFICE PLAN TO CEASE SUPPLYING COPIES OF CITED U.S. PATENT
REFERENCES WITH OFFICE ACTIONS, AND PILOT TO EVALUATE THE
ALTERNATIVE OF PROVIDING ELECTRONIC ACCESS TO SUCH U.S. PATENT
REFERENCES**

Summary

The United States Patent and Trademark Office (Office or USPTO) plans in the near future to: (1) cease mailing copies of U.S. patents and U.S. patent application publications (US patent references) with Office actions except for citations made during the international stage of an international application under the Patent Cooperation Treaty and those made during reexamination proceedings; and (2) provide electronic access to, with convenient downloading capability of, the US patent references cited in an Office action via the Office's private Patent Application Information Retrieval (PAIR) system which has a new feature called "E-Patent Reference." Before ceasing to provide copies of U.S. patent references with Office actions, the Office shall test the feasibility of the E-Patent Reference feature by conducting a two-month pilot project starting with Office actions mailed after December 1, 2003. The Office shall evaluate the pilot project and publish the results in a notice which will be posted on the Office's web site (www.USPTO.gov) and in the Patent Official Gazette (O.G.). In order to use the new E-Patent Reference feature during the pilot period, or when the Office ceases to send copies of U.S. patent references with Office actions, the applicant must: (1) obtain a digital certificate from the Office; (2) obtain a customer number from the Office, and (3) properly associate applications with the customer number. The pilot project does not involve or affect the current Office practice of supplying paper copies of foreign patent documents and non-patent literature with Office actions. Paper copies of references will continue to be provided by the USPTO for searches and written opinions prepared by the USPTO for international applications during the international stage and for reexamination proceedings.

Description of Pilot Project to Provide Electronic Access to Cited U.S. Patent References

On December 1, 2003, the Office will make available a new feature, E-Patent Reference, in the Office's private PAIR system, to allow more convenient downloading of U.S. patents and U.S. patent application publications. The new feature will allow an authorized user of private PAIR to download some or all of the U.S. patents and U.S. patent application publications cited by an examiner on form PTO-892 in Office actions, as well as U.S. patents and U.S. patent application publications submitted by applicants on form PTO/SB08 (1449) as part of an IDS. The retrieval of some or all of the documents may be performed in one downloading step with the documents encoded as Adobe Portable Document format (.pdf) files, which is an improvement over the current page-by-page retrieval capability from other USPTO systems.

Steps to Use the New E-Patent Reference Feature During the Pilot Project and Thereafter

Access to private PAIR is required to utilize E-Patent Reference. If you don't already have access to private PAIR, the Office urges practitioners, and applicants not represented by a practitioner, to take advantage of the transition period to obtain a no-cost USPTO Public Key Infrastructure (PKI) digital certificate, obtain a USPTO customer number, associate all of their pending and new application filings with their customer number, install no-cost software (supplied by the Office) required to access private PAIR and E-Patent Reference feature, and make appropriate arrangements for Internet access. The full instructions for obtaining a PKI digital certificate are available at the Office's Electronic Business Center (EBC) web page at: <http://www.uspto.gov/ebc/downloads.html>. Note that a notarized signature will be required to obtain a digital certificate.

To get a Customer Number, download and complete the Customer Number Request form, PTO-SB125, at: <http://www.uspto.gov/web/forms/sb0125.pdf>. The completed form can then be transmitted by facsimile to the Electronic Business Center at (703) 308-2840, or mailed to the address on the form. If you are a registered attorney or patent agent, then your registration number must be associated with your customer number. This is accomplished by adding your registration number to the Customer Number Request form. A description of associating a customer number with an application is described at the EBC web page at: http://www.uspto.gov/ebc/registration_pair.html.

The E-Patent Reference feature will be accessed using a new button on the private PAIR screen. Ordinarily all of the cited U.S. patent and U.S. patent application publication references will be available over the Internet using the Office's new E-Patent Reference feature. The size of the references to be downloaded will be displayed by E-Patent Reference so the download time can be estimated. Applicants and registered practitioners can select to download all of the references or any combination of cited references. Selected references will be downloaded as complete documents as Adobe Portable Document Format (.pdf) files. For a limited period of time, the USPTO will include a copy of this notice with Office actions to encourage applicants to use this new feature and, if needed, to take the steps outlined above in order to be able to utilize this new feature during the pilot and thereafter.

During the two-month pilot, the Office will evaluate the stability and capacity of the E-Patent Reference feature to reliably provide electronic access to cited U.S. patent and U.S. patent application publication references. While copies of U.S. patent and U.S. patent application publication references cited by examiners will continue to be mailed with Office actions during the pilot project, applicants are encouraged to use the private PAIR and the E-Patent Reference feature to electronically access and download cited U.S. patent and U.S. patent application publication references so the Office will be able to objectively evaluate its performance. The public is encouraged to submit comments to the Office on the usability and performance of the E-Patent Reference feature during the pilot. Further, during the pilot period registered practitioners, and applicants not represented by a practitioner, are encouraged to experiment with the feature, develop a proficiency in using the feature, and establish new internal processes for using the new access to the cited U.S. patents and U.S. patent application publications to prepare for the anticipated cessation of the current Office practice of supplying copies of such cited

references. The Office plans to continue to provide access to the E-Patent Reference feature during its evaluation of the pilot.

Comments

Comments concerning the E-Patent Reference feature should be in writing and directed to the Electronic Business Center (EBC) at the USPTO by electronic mail at eReference@uspto.gov or by facsimile to (703) 308-2840. Comments will be posted and made available for public inspection. To ensure that comments are considered in the evaluation of the pilot project, comments should be submitted in writing by January 15, 2004.

Comments with respect to specific applications should be sent to the Technology Centers' customer service centers. Comments concerning digital certificates, customer numbers, and associating customer numbers with applications should be sent to the Electronic Business Center (EBC) at the USPTO by facsimile at (703) 308-2840 or by e-mail at EBC@uspto.gov.

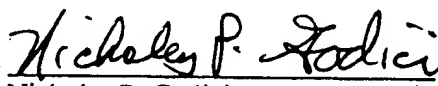
Implementation after Pilot

After the pilot, its evaluation, and publication of a subsequent notice as indicated above, the Office expects to implement its plan to cease mailing paper copies of U.S. patent references cited during examination of non provisional applications on or after February 2, 2004; although copies of cited foreign patent documents, as well as non-patent literature, will still be mailed to the applicant until such time as substantially all applications have been scanned into IFW.

For Further Information Contact

Technical information on the operation of the IFW system can be found on the USPTO website at <http://www.uspto.gov/web/patents/ifw/index.html>. Comments concerning the E-Patent Reference feature and questions concerning the operation of the PAIR system should be directed to the EBC at the USPTO at (866) 217-9197. The EBC may also be contacted by facsimile at (703) 308-2840 or by e-mail at EBC@uspto.gov.

Date. 12/1/03


Nicholas P. Godici
Commissioner for Patents